Communications of the Association for Information Systems

Volume 9 Article 15

October 2002

Wireless Security: An Overview

Robert J. Boncella
Washburn University, zzbonc@washburn.edu

Communications of the Association for Information Systems

WIRELESS SECURITY: AN OVERVIEW

Robert J. Boncella
Washburn University
zzbonc@washburn.edu

ABSTRACT

The physical transport methods used in wireless communication differ from wired communication. These differences affect how a secure channel can be established in a wireless environment. The purpose of this tutorial is to provide an overview of how a secure channel is set up in a wireless environment that uses the 802.11 or WAP standards.

KEYWORDS: WLAN Security, WTLS, WAP, WEP, 802.11b

I. INTRODUCTION

Wireless and mobile networks are rapidly extending their capabilities. In addition to their increasing bandwidth and because of their flexibility and freedom they are becoming the communication infrastructure of choice. Wireless communication provides a user the capability of conducting commerce at anytime, with nearly anyone, from anywhere, using a mobile communication channel. This mobile communication channel can also be used as an access method to the Internet.

As wireless communication and the Internet become truly interoperable, users will want this communication channel to be secure and available when needed. For a message sent using this communication channel, the user expects assurance of:

- *authentication* (the sender and receiver are who they say they are);
- *confidentiality* (the message cannot be understood except by the receiver); and
- *integrity* (the message was not altered).

The goal of this tutorial is to provide an overview of what is required to provide a secure communication channel in a wireless environment. The focus is on the security techniques available for Wireless Local Area Networks (WLAN) and for wireless devices (e.g. cell phones, and PDA's) used to access the Internet.

The tutorial is organized into two main sections. Section II provides an overview of WLAN security as specified in the 802.11 standard. This section also provides a summary of the technology necessary to appreciate the types of security exploits that can be carried out against a wireless network. This discussion assists in understanding WLAN security requirements and their implementation.

Section III summarizes the security problems and solutions when small, low-powered devices try to use low-bandwidth wireless network technology to access services or data-intensive content via the Internet. This section provides an overview of the evolving WAP protocol and its security features.

II. WLAN SECURITY FOR 802.11

WLANs are best suited for home users, small networks, or networks with low security requirements.

With the deployment of wireless networks in business environments, organizations are working to implement security mechanisms that are equivalent to those of wire-based LANs. An additional component of this security requirement is the need to restrict access to the wireless network only to valid users. Physical access to the WLAN is different than access to a wired LAN. Existing wired network have access points, typically RJ45 connectors, located inside buildings which may be secured from unauthorized access through the use of such devices as keys and/or badges. A user must gain physical access to the building to plug a client computer into a network jack.

A wireless access point (AP) may be accessed from off the premises if the signal is detectable. Hence wireless networks require secure access to the AP in a different manner from wired LANs. In particular it is necessary to isolate the AP from the internal network until authentication is verified. The device attempting to connect to the AP must be authenticated. Once the device is authenticated then the user of the device can be authenticated. At this point the user may desire a secure channel for communication.

The 802.11 standard provides the means to satisfy these security requirements - validation of the access device, user authentication and a secure channel. To fully appreciate how these requirements are met an overview of wireless physical transport follows.

WIRELESS PHYSICAL TRANSPORT

The wireless signal that carries the data may be transmitted using electromagnetic waves in the either *radio frequency (RF) or infrared frequency (IR)* portion of the electromagnetic wave spectrum.

If RF Transport is used then the *Spread Spectrum* method is employed to generate the signal. The spread spectrum method expands the initial bandwidth and “spreads it out” in order to use a portion of the expanded bandwidth for portion of the message. Two common variations of the spread spectrum technique are the *Frequency Hopping Spread Spectrum (FHHS) and the Direct Sequence Spread Spectrum (DSSS).*
When the FHSS variation of the spread spectrum is used, non-consecutive portions of the spread spectrum are used to transmit consecutive portions of the message. The transmitted message will be received out of order unless the receiver knows which portion of the spread frequency to tune to and how long to listen before hopping to the next frequency for a specific time period. An analogy would be listening to a song on the radio where the consecutive portions of the song are broadcast sequentially but on different stations. To hear the song correctly the listener would need to tune the stations in the correct sequence. The purpose of using FHSS is security and to reduce signal interference.

When the DSSS method is used, each portion of the message contains additional bits for error correction purposes - the message bits along with its redundant bits is called the “Chip Code” Because of the error correction bits, DSSS reduces the need to retransmit a signal and the result will be a more efficient use of the bandwidth.

If IR transport is used then the signal may be generated either as a *diffused signal* or a *point-to-point signal.*

A *diffused signal* can reflected off of existing surfaces such as a ceiling and that signal can be received by any device within range. A *point-to-point signal* is sent as beam to IR Switch that IR Switch relays the signals to next IR Switch and so forth.

RF is most commonly used of the two physical transport methods. In particular, the 802.11 standard employs the Industrial, Scientific, and Medical (ISM) RF band of the electromagnetic spectrum. This ISM band is specified as:

- the I-Band from 902 MHz to 928 MHz,
- the S-Band from 2.4GHz to 2.48GHz, and
- the M-Band from 5.725GHz to 5.85GHz.

These bands are unregulated since they are used with low power. However, operating at low power limits the distance at which these signals can be detected. For example, depending on circumstances, using the S-band with a bandwidth of 1Mbps the distance varies anywhere from 300 feet indoors to 1500 feet outdoors.

Currently two 802.11 standards are accepted. These are called 802.11b and 802.11a. The earlier standard is the 802.11b and is also referred to as *WiFi (Wire Fidelity).* This standard specifies operation in the 2.4GHz S-band and specifies a max link rate of 11Mbps. A newer standard is 802.11a, also referred to as *WiFi5*. This standard specifies operation in the 5.725GHz M-band and specifies a max link rate of 54Mbps.

Two other variations of the 802 .11 standard are under consideration. The 802.11g which operates in the 2.4GHz S-Band but has a max link rate of 54Mbps and the 802.11i which improves security by means of a stronger implementation of *Wired Equivalent Privacy (WEP)*.

WLAN ARCHITECTURE

A WLAN architecture is built from stations and an access point (AP). The basic structure of a WLAN is the Basic Service Set (BSS). A BSS may either an *independent BSS* or an *infrastructure BSS*.

In an independent BSS, the stations communicate with one another directly if they are within range of each other. These are sometimes referred to as *ad hoc* networks and generally last for a short time. These ad hoc WLANs are typically used for meetings and allow the participants to share data with one another. To participate in an ad hoc WLAN, the participants place the wireless network interface card (WNIC) of their devices into "ad hoc" mode. This mode allows a station to establish a connection with any other station in its proximity.

An infrastructure BSS requires the use of an access point (AP). The AP is used for all communications between stations. If one station wishes to send a transmission to another, the sending station sends its transmission to the AP. The AP then relays this transmission to the receiving station. This transmission requires two hops and will slow the WLAN. However the distance covered by the WLAN is increased by using the AP as a relay device. An important feature of the infrastructure BSS is the need for stations to *associate* to an AP. This feature can be used to set up a WLAN that has a form of restricted access.

Figure 1 illustrates these concepts.

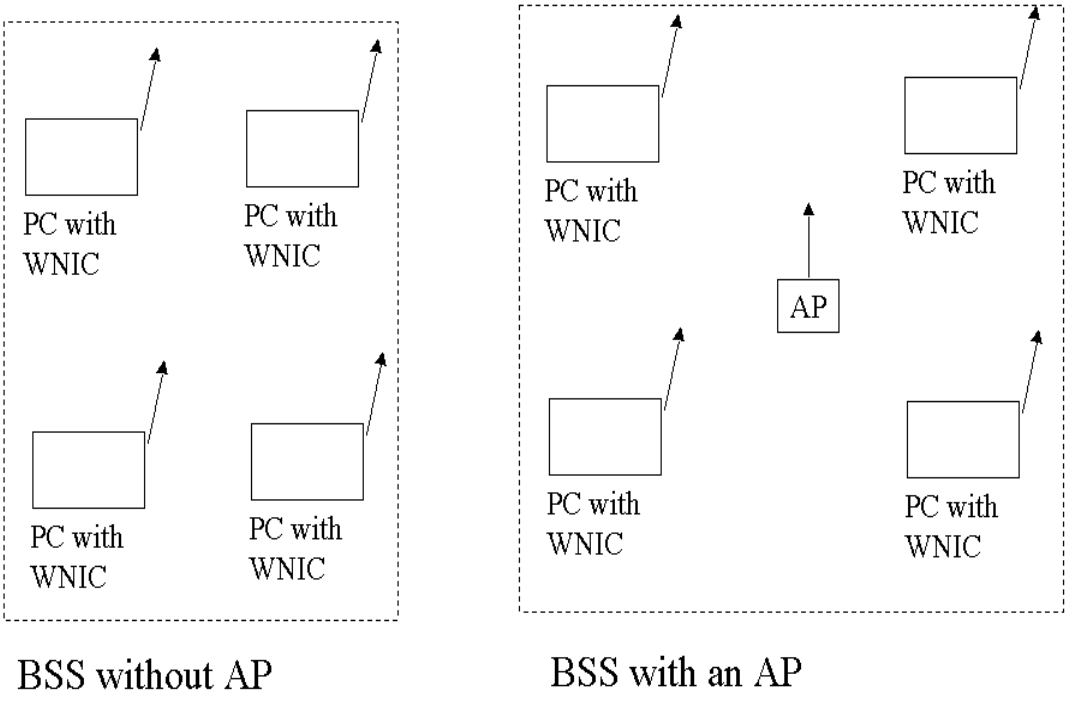

Figure 1 Basic Service Sets With And Without An AP

These BSSs can be combined to form an *Extended Service Set* (ESS).
An ESS is created by chaining together a number of BSSs by using a backbone network. The purpose of an ESS is to allow a station to have *transition mobility*. If a station has transition mobility, a user is able to roam from BSS to BSS and continue to be associated with a BSS and also have access to the backbone network with no loss of connectivity. Figure 2 illustrates this idea.

WLAN SECURITY EXPLOITS

Given the nature of WLANs, a number of security exploits can be carried out against them. The more common exploits are:

Insertion attacks	Interception and unauthorized monitoring	Denial of service (DOS)
Client-to-client attacks	Brute force attacks against AP passwords	Encryption attacks
Misconfiguration		

We now describe each of these exploits:

Insertion Attacks

An insertion attack occurs when an unauthorized wireless client joins a BSS with the intent of accessing the distribution system associated with the ESS that contains the BSS. The intent here is to gain access to the Internet at no cost.

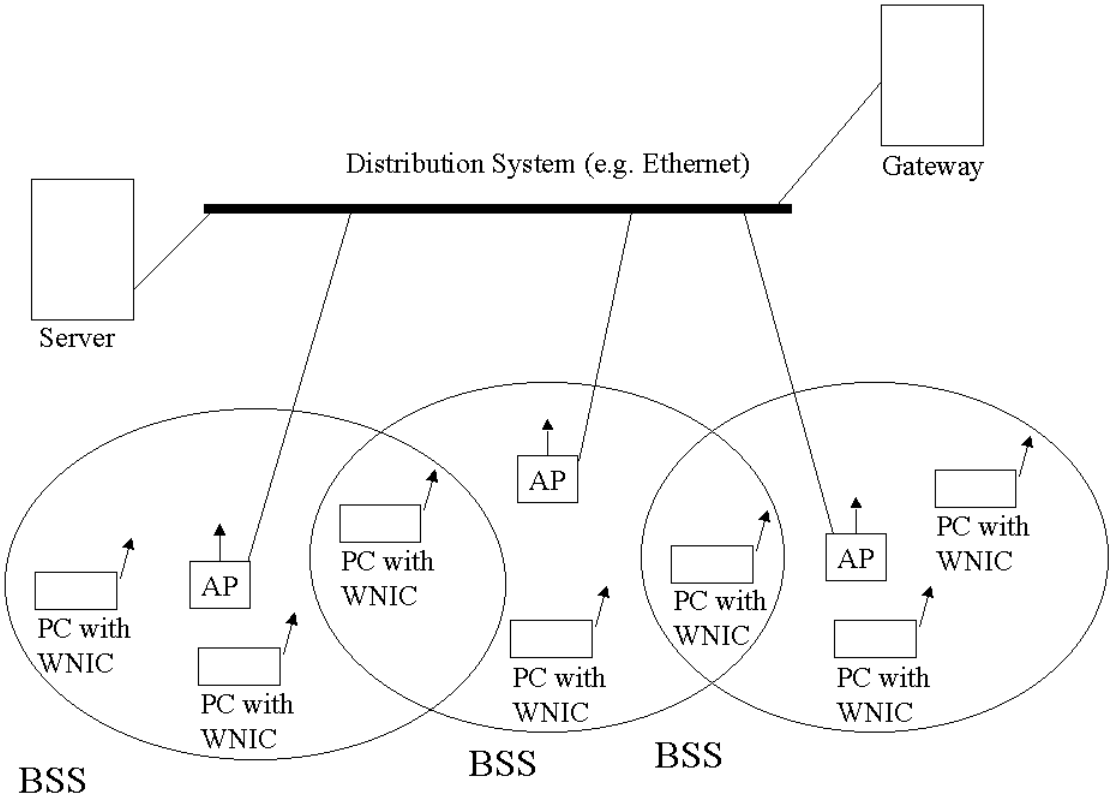

Figure 2 Extended Service Set - ESS

Interception and Unauthorized Monitoring

A wireless client may join a BSS with the intent of eavesdropping on members of the BSS. It is also possible for an unauthorized AP to establish itself as an AP for an Infrastructure BSS. This illegitimate AP acts in a passive role and simply eavesdrops on the traffic among members of the BSS. Under these conditions the person carrying out the exploit can do packet analysis if the packets are not encrypted or traffic analysis if they are encrypted.

Another unauthorized monitoring exploit is broadcast analysis of all the traffic carried on the distribution system. This exploit happens when the distribution system is a hub rather than a switch. In this case all traffic on the hub "shows up" at the wireless AP and both wired packets and wireless are broadcast.

Another insertion attack is to clone a legitimate AP. The effect is to take over the BSS.

Denial of Service (DOS)

Denial of service attacks can be carried out against WLAN by signal jamming. Since the signals are broadcast, it is a somewhat simple matter to jam them. In particular, because of their use of the ISM band, these signals can be jammed using cordless phones, baby monitors, a leaky microwave oven, or any other device that transmits at the ISM band frequencies.

Client-to-Client Attacks

Traditional DOS attacks can be carried out against WLAN by duplicating MAC or IP addresses. The usual TCP/IP service attacks can be carried out against wireless client providing these services (e.g., SNMP, SMTP, FTP).

Brute Force Attacks against AP Passwords

Access to an AP is restricted by means of a password type scheme. This scheme can be compromised by password dictionary attacks.

Encryption Attacks

The packets transmitted from a client to an AP can be encrypted by means of the WEP protocol. This protocol is easily compromised.

Misconfigurations

Most APs ship in an unsecured configuration. The person installing the AP may use the default or factory settings for the AP. For most APs, these values are publicly known and as a result do not provide any security.

BASIC 802.11 SECURITY

To counter these exploits, three basic methods are used to secure access to an AP and provide a secure channel. These are:

- Service Set Identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

One or all of these methods may be implemented, but all three together provide the best solution.

SSID

The *Service Set Identifier (SSID)* is a mechanism that can segment a wireless network into multiple networks serviced by multiple APs. Each AP is programmed with an SSID that corresponds to a specific wireless network segment. This configuration is similar to the concept of a subnet address used in wired LANs. To be able to access a particular wireless network the client computer must be configured with the appropriate SSID. A WLAN might be segmented into multiple WLAN based floor or department. A client computer can be configured with multiple SSIDs for users who require access to the network from a variety of different locations.

A client computer must present the correct SSID to access the AP. The SSID acts as a password and provides a measure of security. This minimal security can be compromised if the AP is configured to “broadcast” its SSID. If this broadcast feature is enabled, any client computer that is not configured with an SSID will receive the SSID and then be able to access the AP. Most often, users configure their own client systems with the appropriate SSIDs. As a result these SSIDs are widely known and easily shared. In addition, an AP may be configured without an SSID and allow open access to any wireless client to associate with that AP.

SSID provides a method to control access to an AP or set of APs . An additional technique that enhances this method is MAC (Media Access Control) Address Filtering.

MAC ADDRESS FILTERING

A client computer can be identified by the unique MAC address of its 802.11 network card. To enhance AP access control each AP can be programmed with a list of MAC addresses associated with the client computers allowed to access the AP. If a client's MAC address is not included in this list, the client will not be allowed to access the AP even if the SSID provided by the client does match the AP's SSID.

This arrangement provides improved security that is best suited to small networks where the MAC address list can be managed efficiently. The management requires that each AP must be programmed manually with a list of MAC addresses. In addition this list must be kept up-to-date. This overhead may limit the size of the WLAN in number of APs and clients devices.

SSID and MAC address filtering satisfy the first of the two requirements of WLAN Security. The requirements of channel security and user authentication are provided by *WEP (Wired Equivalent Privacy)*.

WEP Security

Wireless transmissions are easier to intercept than transmissions in wired networks. In most cases users of WLANs desire secure transmissions. The 802.11 standard specifies the WEP security protocol in order to provide encrypted communication between the client and an AP. WEP employs the RC4 symmetric key encryption algorithm.

When using WEP, all clients and APs on a wireless network use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. Since the 802.11 standard does not specify a key management protocol. All WEP symmetric keys on a network will be managed manually. Support for WEP is standard on most current 802.11 network interface cards and APs. However WEP security is not available in ad hoc (or peer-to-peer) 802.11.

WEP specifies the use of a 40-bit encryption key, although 104-bit keys are also implemented. In either case the encryption key is concatenated with a 24-bit "initialization vector," resulting in a 64- or 128-bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted.

The shared key can be used for client authentication. This requires a four step process between the AP and the client. This process is as follows:

1. the client make an authentication request to the AP;
2. the AP returns a challenge phrase to the client;
3. the client encrypts the challenge phrase using the shared symmetric key and transmits it to the AP;
4. the AP then compares the client's response with its phrase; if there is a match, the client is authorized otherwise the client is rejected.

Compromised WEP Encryption

WEP encryption is vulnerable to attack[1]. Scripting tools exist that can be used to take advantage of weaknesses in the WEP key algorithm to attack a network successfully and discover the WEP key[2] Currently the industry and IEEE are working on solutions to this problem. The Advanced Encryption Standard (AES) is identified as a possible replacement encryption technology for WEP. In addition, revised 802.11 standards (802.11i.and 802.1x) may be adopted which address the security weaknesses of the current standard [Kapp 2002].

Despite the weaknesses of WEP-based security it can be a component of the security solution used in home networks and in small but managed networks with low security requirements. Nonetheless with these networks, 128-bit WEP should be implemented in conjunction with MAC address filtering and SSID. In addition, some sort of WEP symmetric key management should be employed. For example users should change their WEP keys on a regular schedule to minimize risk of compromise.

[1] See http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[2] See http://sourceforge.net/projects/wepcrack.

BEST PRACTICES FOR WIFI SECURITY

Even though it can be compromised, WEP should be used and in particular the 128 bit version. It should be noted that use of WEP will slow down transmission because of the overhead of encryption/decryption process. If WEP is employed then the default key needs to be changed and further the key needs to be changed frequently and randomly. If possible, sessions keys (one time keys) should be used, if available.

Clients should password protect local drives, folders, and files.

The default SSIDs should be changed and the APs should not broadcast their SSIDs.

The APs should use MAC filtering If available.

Finally, to guarantee end-to-end security use a Virtual Private Network. If a network has high security requirements, or will allow many clients, an alternative to the SSID/MAC Address Filtering/WEP protocol is a VPN (Virtual Private Network) solution. VPNs are a mature technology that allows a client to use an "untrusted" network (e.g. the Internet or a wireless network) for secure communication. Briefly this solution requires both a VPN server installed on the network being access by the wireless client and the wireless client having the VPN client software installed .

802.11 SECURITY: SUMMARY

Security problems prevented widespread adoption of 802.11. These problems are related to the design of WEP. Currently the industry is working to solve these problems. It is developing solutions based on the 802.1x specification. The specification is based on the Internet Engineering Task Force's (IETF) Extensible Authentication Protocol (EAP). To be successful 802.1x specifications needs to address two issues associated with the 802.11 standard:

- Guarantee the authenticity and integrity of data frames on a wireless network. Frames are the units of physical transmission in a network. In a wireless network these can be easily intercepted and possibly modified.
- Guarantee the authenticity of the access point (network) to the wireless client. A wireless client needs to be assured that they are attached the intended network. The EAP addresses some of these issues. For details concerning this effort consult [Gast 02].

III. WAP PROTOCOL 1.X

WAP was designed to solve some of the problems caused when small, low-powered devices try to use low-bandwidth wireless network technology to access services or data-intensive content via the Internet. In particular, users want to be able to access e-mail, trade stocks, find out the latest sports scores, or the most recent news event via a cell phone in a secure fashion.

The WAP protocol stack is made up of five layers. These layers are illustrated in Figure 3.

WIRELESS APPLICATION ENVIRONMENT (WAE)

The WAE layer provides an environment to develop and execute applications. In addition it provides services for wireless devices. The WAE layer's primary elements are WML (Wireless Markup Language), a microbrowser, push technology to push data proactively to clients, and multimedia messaging capability.

WIRELESS SESSION PROTOCOL (WSP)

WSP manages the exchange of content. WSP provides applications with a consistent interface for both connection-oriented and connectionless session services. WSP lets client and server applications establish and terminate reliable sessions and agree on common protocols with which

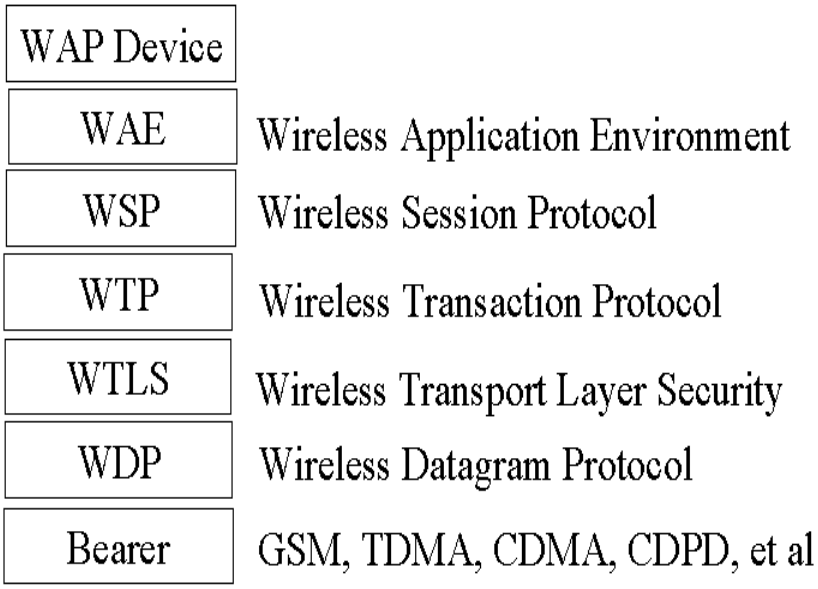

Figure 3 WAP 1.x Protocol Stack

to work. WSP also includes extensions that facilitate wireless transmissions. For example, WSP's compact transmissions. For example, WSP's compact binary headers reduce the overhead and number of transactions necessary to support session services.

WIRELESS TRANSACTION PROTOCOL (WTP)

WTP manages transactions by facilitating requests and responses between a user agent (such as a WAP microbrowser) and an application server for such activities as browsing and e-commerce transactions. WTP works well in the low-bandwidth wireless environment because it requires the wireless device and the gateway to send each other relatively few packets to manage or maintain the connection. WTP can provide data streaming, hypermedia, and message transfer.

WIRELESS TRANSPORT LAYER SECURITY (WTLS)

WTLS secures, authenticates, and encrypts data transmissions between the WAP gateway and mobile devices. To support mobile networks, WTLS was designed to be more efficient than SSL, which requires client and server to exchange many messages. In wireless networks, which frequently experience considerable latency, this requirement can slow response time significantly. WAP systems translate WTLS data to SSL data for transmission over the Internet within the WAP gateway.

WIRELESS DATAGRAM PROTOCOL (WDP)

WDP lets WAP support many network technologies. WAP works with the major wireless network technologies used in different parts of the world, including CDMA (code-division multiple access), GSM (global system for mobile communication), and TDMA (time-division multiple access). WAP also supports the major operating systems used in handheld devices (e.g. JavaOS, PalmOS, and Windows CE). When working with IP bearer services, WDP functions just like the User Datagram Protocol. With non-IP bearer services, such as CDMA, WDP performs the adaptation necessary to carry transmissions.

WAP AND INTERNET ACCESS

WAP uses proxy technology to connect wireless technology with the Web. The WAP proxy server consists of a gateway, encoders, and decoders. The gateway translates requests from the WAP protocol stack to the WWW stack so they can be submitted to Web servers. Encoders and decoders translate WAP content into compact encoded formats that reduce the amount of data being sent over the low-bandwidth wireless network. Wireless technology's bandwidth and latency constraints cannot support the Internet standards of HTML, HTTP, IP, TCP, and TLS (transport layer security). These are inefficient over mobile networks. For example, HTTP sends its headers in text format, instead of compressed binary format. Meanwhile, to work with HTTP and HTML, machines must have fast network connections, powerful processors, and large memories, components not currently found in handheld devices. This proxy technology is shown in Figure 4.

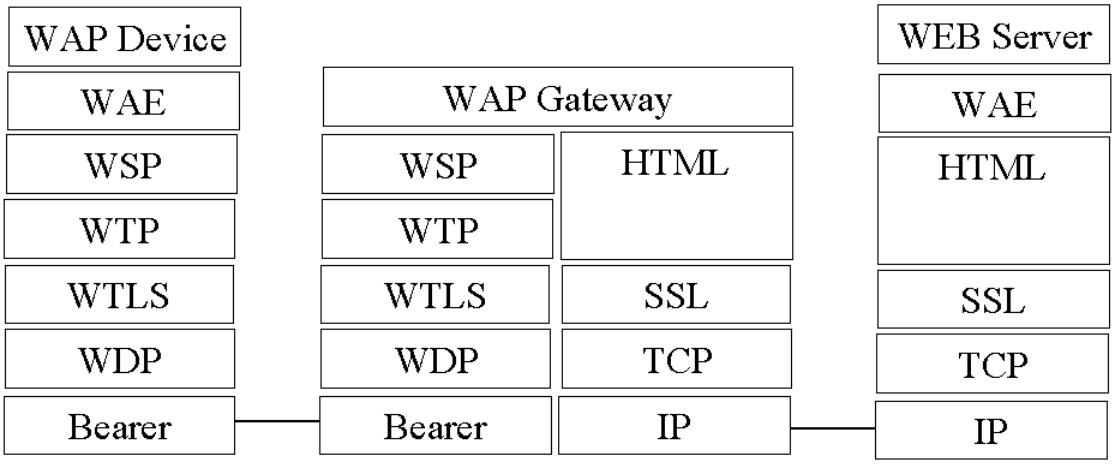

Figure 4 WAP 1.x Gateway

WAP 1.X SECURITY

The layer of the WAP protocol that provides security is the WTLS layer. WTLS functions similar to SSL (also known as Transport Layer Security (TLS)). WTLS provides for server and/or client authentication via certificates similar to X.509 certificates. WTLS also allows for the negotiation of encryption parameters between the client and server, thus ensuring a secure channel for communication. Although WTLS does not provide end-to-end security, the chances of a problem are small because hackers can breach security only when sensitive data passes through the WAP gateway. WTLS provides the security necessary to conduct e-commerce on handheld wireless devices.

WAP PROTOCOL 2.0

In January, 2002 the WAP Forum released version 2.0 of the Wireless Application Protocol - http://www.wapforum.org/what/WAPWhite_Paper1.pdf.

WAP 2.0 extends bearer services to include GPRS (General Packet Radio Service) and 3G (3rd Generation) cellular, thus providing access to higher bandwidth and speeds. Because it provides these extend services WAP 2.0 contains support for the standard Internet protocols of IP, TCP and HTTP.

To interoperate with these Internet Protocols, the WAP 2.0 Protocol stack contains:

1. WP-HTTP (Wireless Profiled HTTP) - A profile of HTTP for wireless environment that is interoperable with HTTP/1.1;
2. TLS (Transport Layer Security) - a profile of the TLS protocol that will allow for secure transactions and provide for end-to-end security at the transport layer. This capability is similar to what wire users expect with the SSL layer; and
3. WP-TCP (Wireless Profiled TCP) WP-TCP will provide connection-oriented services.

The WAP 2.0 enabled device now contains the following layers depicted in Figure 5.

As a result, a WAP 2.0-enabled device will be able to interact efficiently with a wired web server through a WAP Proxy which only contains only the wireless to wired, IP to IP, TCP to TCP layers.

Finally, to remain backward compatible with existing WAP 1.x applications, newer WAP devices will support both stacks (WAP 1.x and WAP 2.x) independently. As a result the WAE layer will be accessible to both stacks.

WAP 2.0 SECURITY

Since WAP 2.0 includes a version of TLS (Transport Layer Security) in its WAP Device stack, version 2.0 security is improved over version 1.x. In particular the WAP proxy no longer needs to translate the WTLS protocol into the TLS protocol when sending data to a wired web server and visa versa. Overall WAP 2.0 provides better end-to-end security. These changes are shown in Figure 6.

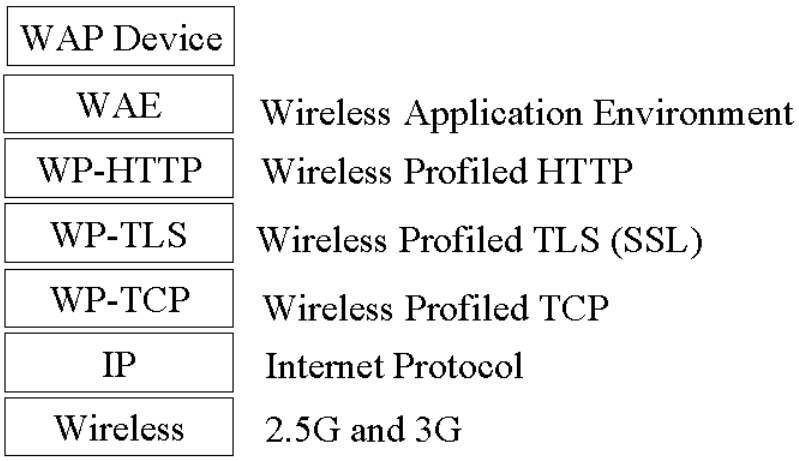

Figure 5 WAP 2.x Protocol Stack

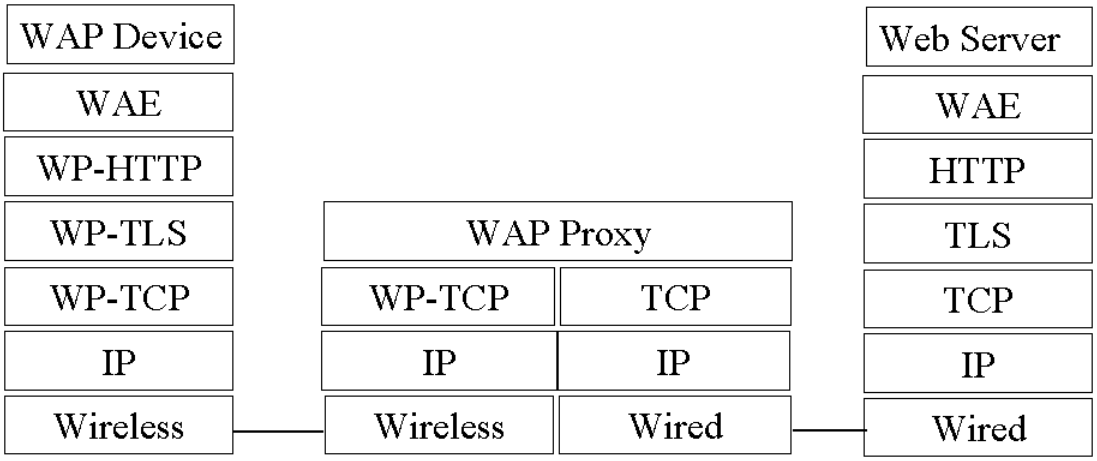

Figure 6 WAP 2.0 Proxy

Editor's Note: This article is based on a tutorial given at AMCIS 2002 in Dallas TX. The article was received on September 8, 2002 and was published on October __ 2002.

BIBLIOGRAPHY

Dornan, A. "LANs with No Wires, but Strings Still Attached", *Network Magazine*, (17)2, 2002, pp. 44-47.

Dornan, A. "Fast Forward to 4G?", *Network Magazine*, (17)3, (2002) 3, pp. 34-39.

Fratto, M. "Tutorial: Wireless Security", *Network Computing*, Jan. 22, 2001, http://www.networkcomputing.com/1202/1202f1d1.html

Garber, L. "Will 3G Really Be the Next Big Wireless Technology?", *IEEE Computer*, (35) 1, 2002, pp.26-32.

Gast. Matthew S. *802.11 Wireless Networks: The Definitive Guide* O'Reilly & Associates Inc., Sebastopol, CA (2002).

Kapp, S. "802.11: Leaving the Wire Behind", *IEEE Internet Computing Online"*, January/February 2002, http://www.computer.org/internet/v6n1/w102wire2.htm.

Internet Security Systems. "Wireless LAN Security: 802.11b and Corporate Networks", 2001, http://www.iss.net/support/documentation/otherwhitepapers.php

Macphee, Allan "Understanding Digital Certificates and Wireless Transport Layer Security (WTLS)", *Entrust Whitepaper*, 2001
http://www.entrust.com/resources/whitepapers.htm

Nichols, R. K., and Lekkas, P. C., *Wireless Security: Models, Threats, and Solutions*, New York, NY: McGraw-Hill, 2002.

Varshney, U. and Vetter, R. "Emerging Mobile and Wireless Networks", *Communications of the ACM*, (43) 6, 2000, pp. 73-81. (2002)

WAP Forum., "Wireless Application Protocol WAP 2.0", *WAP Forum Technical White Paper*, 2000, http://www.wapforum.org/what/WAPWhite_Paper1.pdf .

ACRONYMS

AES Advanced Encryption Standard
AP Wireless Access Point
BSS Basic Service Set
CDMA Code Division Multiple Access
DOS Denial of Service
DSSS Direct Sequence Spread Spectrum
EAP Extensible Authentication Protocol
ESS Extended Service Set
FHHS Frequency Hopping Spread Spectrum
GPRS General Packet Radio Service
GSM Global System for Mobile Communication
HTML Hypertext Markup Language
HTTP Hypertext Transfer Protocol
IETF Internet Engineering Task Force
IP Internet Protocol
IR Infrared
ISM Band Industrial, Scientific and Medical RF Band
MAC Media Access Control
RC4 Ron's Code Four
RF Radio frequency
SSID Service Set Identifier
SSL Secure Sockets Layer
TCP Transport Layer Protocol
TDMA Time Division Multiple Access
TLS Transport Layer Security
VPN Virtual Private Network
WAP Wireless Application Protocol
WEP Wired Equivalent Privacy
WiFi Wire Fidelity
WLAN Wireless Local Area Network
WNIC Wireless Network Interface Card

ABOUT THE AUTHOR

Robert J. Boncella (http://www.washburn.edu/cas/cis/boncella) is Professor of Computer Information Science at Washburn University, Topeka, KS. Dr. Boncella has a joint appointment in the Computer Information Sciences Department, where he conducts classes in Data Communications and Computer Networks, and in the School of Business, where he offers instruction on Computer Based Information Systems in the school's MBA program. He holds a Ph.D. and Masters degrees in Computer Science from the University of Kansas and a Master of Arts in Philosophy from The Cleveland State University. He is a member of ACM, AIS, AAAI, and IEEE. His current areas of interest are web based information systems, intelligent agents and decision making under uncertainty as well as computer security and privacy.

ISSN: 1529-3181